Kombinasi Nilai Indeks pada Skema Eksaminasi Menggunakan Fungsi Logistik Sebagai Pembangkit Bilangan Acak (Suatu Kajian Pencarian Bilangan Acak Terbaik)

Hanna Widhi Pratama[1], Alz Danny Wowor[2]

Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Jl. Diponegoro52-60, Salatiga 50711, Indonesia
Email : 672013136@student.uksw.edu[1] , alzdanny.wowor@staff.uksw.edu[2]

Abstract

Cryptography is currently used as a information security, every days information which characteristic as a secret information are vulnerable to attacks. With the existence of cryptography, information that was originally in the form of plaintext will be processed into a ciphertext in order that not everyone knows the contents of the information and if there is a leak against the ciphertext it will be difficult to solve. This research will design a scheme that can maintain security of the information. Using this examination scheme it can generate keys as random numbers to produce different ciphertexts every time you enter the same plaintext and key input. This scheme will certainly guarantee multiple security from ordinary algorithms. By using a 256-bit random number generator, iteration equation, key test with runs up and down test, the best correlation test which is carried out key to each plaintext to produce the best encrypted data encryption. The resulting ciphertext will be very different from the inputted plaintext, it maybe seen like not having a relationship between input (plaintext) and processed results (ciphertext). The results that have been done from plaintext A input produce 3 ciphertexts which are dec2hec numbers with the best randomness.

Keyword *:Cryptography, Examination Scheme, Iteration, Reverse Random Number*

Abstrak

Kriptografi saat ini digunakan sebagai pengamanan informasi, semakin hari informasi yang bersifat rahasia semakin rentan terhadap serangan. Dengan adanya kriptografi, informasi yang semula berupa plainteks akan diproses menjadi sebuah cipherteks dengan tujuan tidak semua orang mengetahui isi informasi tersebut dan bila terjadi kebocoran terhadap cipherteks akan sulit untuk dipecahkan. Penelitian ini akan merancang sebuah skema yang dapat menjaga keamanan informasi tersebut. Dengan menggunakan skema *examination* ini dapat membangkitkan kunci sebagai bilangan acak untuk menghasilkan cipherteks yang berbeda setiap melakukan masukan plainteks dan kunci yang sama. Skema ini tentu akan menjamin keamanan berlipat dari algoritma biasa. Dengan menggunakan pembangkit bilangan acak 256 bit, persamaan iterasi, uji kunci dengan *runs up and down test*, uji korelasi terbaik yang dilakukan kunci terhadap masing-masing plainteks untuk menghasilkan enkripsi ciperteks terbaik secara acakannya. Cipherteks yang dihasilkan akan berbeda jauh dengan plainteks yang diinputkan, ketika dilihat seperti tidak memiliki hubungan antara inputan (plainteks) dengan hasil olahan (cipherteks). Hasil uji yang telah dilakukan dari *input* plainteks A menghasilkan 3 cipherteks berupa bilangan *dec2hec* dengan keacakan terbaik.

KataKunci : Kriptografi, Skema Examination, Iterasi,bilangan acak terbaik

---

[1]Mahasiswa Program studi Teknik Informatika Fakultas Teknologi Informasi Universitas Kristen Satya Wacana

[2]Staff pengajar Fakultas Teknologi Informasi Universitas Kristen Satya Wacana Salatiga